OSEC

Know your tools: OpenSSH

Dariusz Puchalak

- 20+ lat Linux/Unix Sysadmin
- 9+ lat trener
- 2+ lat w OSEC

http://www.OSEC.pl

- 7+ lat na rynku
- doświadczona kadra (ACNI, RHCA)
- specjalizacja open-source
- subskrypcje, szkolenia, konsultacje

OpenSSH changes

OpenSSH 6.5

- Curve25519 - key exchange using elliptic-curve Diffie Hellman
- Ed25519 - elliptic curve signature scheme
- chacha20-poly1305@openssh.com - ChaCha20 stream cipher and Poly1305 MAC
- Refuse RSA keys from old proprietary clients and servers that use the obsolete RSA+MD5 signature scheme
- Refuse old proprietary clients and servers that use a weaker key exchange hash calculation
- new private key format that uses a bcrypt KDF

OpenSSH 6.5 - client

- Increase the size of the Diffie-Hellman groups requested for each symmetric key size. New values from NIST SP 800-57
- Match

OpenSSH 6.5

- Released: ???

OpenSSH 6.5

- Released: 2014-01-30

Najgłośniejsze wydarzenie roku 2013

?

Najgłośniejsze wydarzenie roku 2013

Global surveillance disclosures

by Edward Snowden

OpenSSH Server

- UseDNS now defaults to 'no' - 6.8
- Fingerprints new format: SHA256:9IBSXO8EpQ+Jz+8GKjixM4/hw/Jg7+GwnHXc/7aUtJY – 6.8
- DisableForwarding - disables X11, agent, TCP, tunnel and Unix domain socket forwarding, as well as anything else we might implement in the future. - 7.3

OpenSSH Server

- Disable SSH v1 - 7.4
- Disable pre-authentication compression - 7.4
- forced-command in both a certificate and an authorized keys/principals command= restriction sshd will now refuse to accept the certificate unless they are identical - 7.4
- Only with privilage seperation - 7.5+

OpenSSH Client

- Increase the size of the Diffie-Hellman groups requested for each symmetric key size. New values from NIST SP 800-57 - 6.5
- Match - 6.5
- Unix domain socket forwarding – 6.7

OpenSSH Client

- ProxyJump - 7.3
- IdentityAgent - overrides SSH_AUTH_SOCK - 7.3
- Include - Include the specified configuration file(s). - 7.3

OpenSSH Client

- proxy multiplexing mode to ssh – 7.4
- Remove (from proposal) 3des-cbc - 7.4
- ssh-agent refuse to load PKCS#11 modules outside a whitelist of trusted paths by default - 7.4
- SSHv1 - 7.5+

OpenSSH ssh-keygen – 7.3

ssh-keygen(1): allow fingerprinting multiple public keys in a file,

```
puchalakd@www:~$ ssh-keygen -lf ~/.ssh/authorized_keys
1536 SHA256:9lBSXO8EpQ+Jz+8GKjixM4/hw/Jg7+GwnHXc/7aUtJY kluczyk1 (RSA)
1536 SHA256:JLZXs8S+GqYx3HSaqsIAgj27U9omV7x8EuOLD9WbjIU kluczyk2 (RSA)
```

OpenSSH server

- PermitUserRC - 6.7
- new authorized_keys option "restrict" that includes all current and future key restrictions (no-*-forwarding, etc.) - 7.3
- Also add permissive versions of the existing restrictions, e.g. "no-pty" -> "pty" - 7.3

Fuck ups...

?

UseRoaming

?

UseRoaming

- Information Leak (CVE-2016-0777) - Private Key Disclosure
- Buffer Overflow (CVE-2016-0778)

- Version: 5.4 - 7.1.p2
- Mitigation: UseRoaming no

Miłe dodatki.

ssh-keygen

- Generowanie pary kluczy.
- Zalecane algorytmy (-t) : rsa, ed25519
- Zalecany nowy format klucza (-o) dla OpenSSH >= 6.5
- Łatwe zarządzanie know_hosts
  - ssh-keygen -f "/home/puchalakd/.ssh/known_hosts" -R 192.168.100.179

AutorizedKeysCommand

- Pobieranie authorized_keys za pomocą komendy.
- AuthorizedKeysFile
- AuthorizedKeysCommand
- AuthorizedKeysCommandUser (dedykowane konto)

PKI

- OpenSSH CERTIFICATES
- AuthorizedPrincipalsFile
- TrustedUserCAKeys
- RevokedKeys

PKI

- KEY REVOCATION LISTS (format)
- CERTIFICATES format

2FA authentication

- AuthenticationMethods publickey,password publickey,keyboard-interactive
- AuthenticationMethods publickey,publickey

Match

- User
- Group
- Host
- LocalAddress
- LocalPort
- Address
- All

Match

AcceptEnv, AllowAgentForwarding, AllowGroups, AllowTcpForwarding, AllowUsers, AuthenticationMethods, AuthorizedKeysCommand, AuthorizedKeysCommandUser, AuthorizedKeysFile, AuthorizedPrincipalsFile, Banner, ChrootDirectory, DenyGroups, DenyUsers, ForceCommand, GatewayPorts, GSSAPIAuthentication, HostbasedAuthentication, HostbasedUsesNameFromPacketOnly, KbdInteractiveAuthentication, KerberosAuthentication, MaxAuthTries, MaxSessions, PasswordAuthentication, PermitEmptyPasswords, PermitOpen, PermitRootLogin, PermitTTY, PermitTunnel, PermitUserRC, PubkeyAuthentication, RekeyLimit, RhostsRSAAuthentication, RSAAuthentication, X11DisplayOffset, X11Forwarding, X11UseLocalHost.

Tożsamości

```
Host s1.puchalak.net
    IdentityFile ~/.ssh/s1.key
    IdentitiesOnly yes
```

Wildcards

```
Host s??w.puchalak.net
    IdentityFile ~/.ssh/show.key
    IdentitiesOnly yes
    User rootdp
```

Match po stronie klienta

- exec
- host
- originalhost
- user
- localuser
- All

Match po stronie klienta

```
Match host sun exec "ping -c 1 -W 1 192.168.1.1"
        Hostname 192.168.0.45


Host sun
        Hostname 1.2.3.4
        Port 2024
        ProxyCommand ssh ovh-https nc %h %p
```

Ansible – my new best toy.

```
ControlMaster auto
ControlPath ~/.ssh/ControlPath/%C
ControlPersist 1200
```

BetterCrypto

https://bettercrypto.org

Pytania?
Dariusz.Puchalak@osec.pl